3

ARTICLE APPEARED ON PAGE A19

NEW YORK TIMES
27 June 1985

Move Into World of Computer Nets By Intelligence Unit Raises Doubt

By DAVID BURNHAM
Special to The New York Times

WASHINGTON, June 26 — As computer and communications technologies advance, the nation's largest intelligence agency has become involved in keeping foreign powers, private corporations and criminals from electronically eavesdropping on the computer and communication networks of Government and private institutions.

Because data bases and communication systems are crucial to their owners' independence and control, the role of the National Security Agency has led to disputes in the Government and prompted questions from members of Congress and other groups.

Since 1952 the security agency, with a current budget reported at more than $4 billion a year, double that of the Central Intelligence Agency, has been responsible both for conducting worldwide electronic surveillance and protecting the important messages of the United States from interception.

Under an order issued by President Reagan last September, the agency is now working to place secure telephones on hundreds of thousands of desks of Government officials and executives in industries that deal with the military. In addition, the agency has concluded an agreement with the Treasury Department to improve protection of the electronic transfer of Government money and has begun an effort to persuade computer manufacturers to produce a device at relatively low cost to encode information flowing in and out of computer data bases.

House Hearing to Be Held

On Thursday a House Science and Technology subcommittee headed by Representative Dan Glickman of Kansas, a Democrat, plans hearings on implications of the agency's new role. This will be one of the first public Congressional examinations of the agency since illegal surveillance work by the agency was disclosed almost 10 years ago by the Senate Intelligence Committee.

Representative Glickman said in an interview that there were "very broad policy implications involved in allowing the Department of Defense and the intelligence community to set policy for the Government's civilian agencies and the private sector in a very sensitive area."

The Congressman said three questions should be examined: Who is the master of the agency, which is nominally under the Department of Defense; what tasks should it undertake and is there enough evidence of eavesdropping to support spending hundreds of millions of dollars on improved security?

Since the agency's earliest days, according to experts on the subject in Congress and elsewhere, there have been conflicts because the Secretary of Defense and the Director of Central Intelligence share responsibility for the agency's direction.

Conflicts Are Magnified

But nearly all the knowledgeable officials agree that these conflicts have been magnified by Mr. Reagan's decision to expand the agency's role from the relatively narrow area of communication security into computer security.

Senior officials in the agency and the Pentagon and experts in both the House and Senate said a battle over the wording of the Reagan order, National Security Decision Directive 145, was one element in an intense struggle between Lieut. Gen. Lincoln D. Faurer, then head of the agency, and the Deputy Secretary of Defense, William Howard Taft 4th.

They said the dispute was symptomatic of the many contradictions and conflicts concerning the agency.

One central difference concerns a provision in the directive making the National Security Agency the "national manager" for research on computer and telephone security.

For instance, one Pentagon scientist with many years of experience in computer security said: "The Strategic Air Command doesn't want anyone, including the N.S.A., learning about how it goes about securing its computers and the secrets it stores in them.

Another part of the dispute over the wording of the directive centered on whether it impinged on the structure that maintains control of the various intelligence agencies as they go about the jobs assigned to them.

Early drafts of the directive, for example, increased the authority of the agency to report directly to the White House National Security Council. "This did not sit well with Defense Secretary Weinberger, the N.S.A.'s nominal boss," said one Congressional staff member familiar with the struggle. "He raised hell and this section was deleted."

Some experts doubt that the United States needs all the broad programs for communication and computer security being pursued by the agency.

For example, last July, in a letter to Richard G. Stilwell, the deputy Under Secretary of Defense for policy, for example, the heads of the Aerospace Industries Association and the Electronic Industries Association questioned one Pentagon project. The two private trade assocations said it "appears to be focused on broad generic vulnerability instead of on discernible threats" and recommended a narrower approach.

Many other experts, however, believe that the United States has already suffered harm because it lacks a workable arrangement to provide security in the computer age.

Under the authority of Directive 145, the agency is moving swiftly into its new role. Two months ago it announced it would give three huge communication companies $44 million in the next few years to encourage them to create a secure telephone to end most international and corporate telephone eavesdropping.

The agency hopes the new instruments, which are expected to cost less than $2,000 each, will become standard in 500,000 Government and corporate offices in five years.

About the same time the agency was designating the three, American Telephone and Telegraph, RCA and Motorola, for this job, it also signed an agreement with the Treasury Department and the National Bureau of Standards to improve security for the $500 billion yearly in Government collections and payments now moving by computer network.

In a recent interview, the agency's communication security chief, Walter G. Deeley, said he was negotiating with computer manufacturers to develop a low-cost device to encode the information stored in most computers. Mr. Deeley said the Government now purchases a relatively small number of these devices each year for $10,000 each. If the technology went into mass production and the devices were widely used, he said, the cost could drop to $200 a unit.